## ABSTRACT OF THE DISCLOSURE

The Evidentiary Imaging System (EIS) provides secure storage or transmission of a digital image into which is encoded the date, time, and location at which the image was taken, along with the camera ID and frame number. The encoding is dispersed throughout the image so that the image cannot be modified without distorting the encoding. The image may be encrypted for additional security. Annotation can be superimposed on the encoded or encoded and encrypted image to classify or identify the image to human or automated scanning systems. The annotation can also be used to key the decoding and decryption tasks. The EIS produces imagery which may be authenticated as to originality, time and location of imaging. The imagery may be stored, duplicated, and transmitted while retaining its authenticity. However, any modifications to the image, including any local changes, are readily detected because the encoding will not decode correctly. The EIS is designed to provide imagery which may be used for evidentiary proof of authenticity, ownership, originality, date and time, and location of imaged events. Certain users of EIS systems, such as police forensics labs, may have a central depository for the decoding and decryption keys used with their cameras. Other users may rely upon authentication services provided by the EIS manufacturer or an independent expert in the EIS technique.

While many different schemes for encoding and encryption may be used, FlashCorrelation® provides a computationally simple and rapid method for encoding each item of information;  allowing for separate or total encoding and readout of encoding layers representing: date, time, location, camera ID, and frame number.  As covered in the issued FlashCorrelation® patents 5,583,950 and 5,982,932, readout and authentication can be done by one party authorized to have the decoding and decryption schemes, or readout and authentication may require two or more parties.